Minimum Security Standards

DRAFT

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
1	**Computer Room Physical & Environmental Controls**				
1.1	All server and network equipment is located in a controlled-access area(s) that have physical restrictions on entry, to supporting staff only. If a controlled-access area is not available, equipment is enclosed in locked racks.				
1.2	Unauthorized employees or vendors are logged and escorted in controlled-access area(s).				
1.3	Controlled-access areas display no signage indicating they are a computer facility but still comply with all legally mandated signage requirements.				
1.4	A UPS (uninterrupted power supply) having sufficient battery time to prevent data loss is in place and functional.				
1.5	Smoke, water, fire, and high/low temperature detection devices are operational in any unmanned, controlled-access areas.				
1.6	Escalation procedures are in place in the event of an issue in the controlled-access area.				
2	**User Authentication & Access Controls**				
2.1	Access to computing and network resources is only granted upon written request approved by the manager or supervisor of the requestor. When an incident management tool is not used, the request process is documented in writing and periodically validated.				
2	**User Authentication & Access Controls**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
2.2	Individual UserIDs all conform to a standard format. Generic UserIDs are only used in the case of "Service Accounts/programmatic access."				
2.3	User IDs are deactivated after a 30-day period of inactivity and all associated privileges revoked. IDs are reviewed for deletion after 60 days unless written management direction exists to extend the period.	Domain and System User IDs are deactivated after a 30-day period of inactivity. IDs are reviewed for deletion after 60 days. Deactivation or deletion may be extended by written management approval.			
2.4	Domain login passwords have a minimum length of 8 characters with complexity enforced to include upper case, lower case, numbers, and special characters, wherever possible. Admin. passwords should also include 1 special character whenever possible.	Domain login passwords have a minimum length of 8 characters with complexity enforced to include upper case, lower case, and numbers.~~, and special characters, wherever possible.~~ Admin. passwords also include 1 special character, whenever possible. For system passwords that don't authenticate against domain access controls, passwords are managed as closely to domain complexity as possible, or as the device will allow.			
2.5	Third-party vendors are not given external access privileges to court servers and/or networks without a business-requested, justifiable need. Privileges are enabled only for the time period required to accomplish the approved tasks or the contract time period, whichever is shorter.				
2.6	User and service account (non-user) passwords are changed at least once every 90 days. Any service accounts having a greater than 90 day change cycle are documented with signed management approval.	System and Domain User or service account (non-user) passwords are changed at least once every 90 days. Any system or service accounts having a greater than 90 day change cycle are documented with management approval.			
2	**User Authentication & Access Controls**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
2.7	Passwords are never stored in readable form in locations where unauthorized persons could discover them. Sharing passwords between users is prohibited.				
2.8	Initial passwords, or passwords that have been reset by an administrator, are changed to a unique password at first login. No password is reset without positive verification of the identity of the account holder.	On capable systems, initial passwords, or passwords that have been reset by an administrator, are changed to a unique password at first login. No password is reset without positive verification of the identity of the account holder.			
2.9	To prevent password guessing, all computing and network devices requireing passwords are limited to 3 incorrect attempts prior to being disabled from use.	To prevent password guessing, all computing and network devices requireing passwords are limited to 3 incorrect attempts prior to being disabled from use on capable systems.			
2.10	Every password on a system is changed at the time of the next log-in whenever system security has been compromised or there is a convincing reason to believe it has been compromised.	Every password on a given system is changed, at the time of the next log-in, whenever that system security has been compromised or there is a convincing reason to believe it has been compromised.			
2.11	Authoritative outside contacts inform court management of the termination of any computer or network user prior to or immediately upon termination.				
2.12	System privileges granted to users are reevaluated by local management periodically and in response to changes in job role. When informed by management, system admins promptly revoke all privileges no longer needed by users.	System access granted to users are reevaluated by local management periodically and in response to changes in job role. When informed by management, system admins promptly revoke all user access no longer needed by users.			
2	**User Authentication & Access Controls**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
2.13	Termination of an employee with "Admin" system access results in immediate password change to all systems.				
2.14	Upon termination of an employee, the immediate manager determines the custodian of the employee's files and/or the appropriate methods to be used for disposal. Unless directed otherwise in writing, 4 weeks after termination, all files held in that user's personal folders are purged.				
2.15	User Authentication and Access Controls on newly deployed environments, that are managed at the Application Layer, must conform to the standards for password aging and format. Legacy environments, that are unable to comply, need to have management acknowledgement of the risk and a plan for mitigation.				
3	**External Access to the Court Network**				
3.1	VPN connections to court domains and/or server systems pass through an access control point/firewall before users employing these connections reach a log-in banner.				
3.2	User-based communication access between court network users and external resource environments occurs only by direct access through a court firewall. This may also include a one-way domain trust for user authenication.				
3	**External Access to the Court Network**				
3.3	Programmatic access into the court network is permitted only via network edge firewalls, VPN, or IBM MQ IPT front end.				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
3.4	All server and client devices accessing the court network have up-to-date anti-virus protection on them. Anti-virus programs are protected against user access and never disabled.				
4	**Court Computing and Network Devices**				
4.1	Confidential or restricted information is appropriately classified at its source.				
4.2	All "confidential " or "restricted" information transmitted over any communication network other than the court network is only sent in an encrypted form.				
4.3	All Web-based devices and printers communicating outside of the court network only do so using TLS and have an authenticated certificate installed.				
4.4	All domain-attached servers and workstations have approved anti-virus screening software enabled on their computers at all times. Users can not disable or deactivate this software.				
4.5	All downloaded files from non-Judicial-Branch sources are screened with virus detection software prior to being opened/saved/executed.				
4	**Court Computing and Network Devices**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
4.6	No local subdomains, web servers, new local area networks, backdoor connections to existing local area networks, or other equipment used for data communication are attached to the court network without specific approval from the network management organization.				
4.7	All PCs employ a locking screen saver program which requires a password to access. Timeout is set to no longer than 15 minutes of inactivity for any public accessible device including all laptops; 60 minutes for devices within any locked area by approval of court leadership; and no timeout restrictions for pre-defined single-application courtroom devices or public access devices employing other security methods.				
4.8	User shares and general shared folders do not default to read, write, and execute for anonymous users. Shares are restricted to specific domain users and/or groups.				
4.9	Web sites that contain sexually explicit racist, violent, or other potentially offensive material are blocked using third-party lists, updated frequently.				
4.1	Computer and communications systems handling Judicial Branch information log all user connections for forensic purposes. Systems that connect to AJCIS follow current DPS and FBI access logging requirements.	Computer and network communications systems handling Judicial Branch information log all user connections for forensic purposes.			
4	**Court Computing and Network Devices**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
4.11	User access logs are retained for at least 30 days onsite and secured such that they cannot be modified and can be read only by authorized persons.	User connection logs are retained for at least 30 days onsite and secured such that they cannot be modified and can be read only by authorized persons.			
4.12	All network intrusion detection is done through the court's network services organization. Detection logs are backed up and retained for a 30-day window.	All network monitoring and data capture of any courts data/traffic should be performed by the court's network services organization. Any monitoring outside of the courts network services organization should be authorized by the court and given access to the monitoring for oversight. Data should be stored for a minimum of 30 days. (AOC network is the authoritative network service organization for AJIN)			
4.13	All computer and network devices are maintained with the latest vendor-provided security updates available for the specific O/S.				
4.14	Security audit scans of all computing devices in all domains occur not less than twice per year. Reports are distributed to local administration staff. Information technology or network management defines those vulnerabilitiies that must be remediately immediately.				
4.14	Notification of any new server or printer being added to the court network is communicated to the information technology manager via a defined process prior to being commissioned.				
4	**Court Computing and Network Devices**				

Minimum Security Standards

#	Requirements or Control	Post-TAC Modified Req't	Currently Meets	Explanation	Plan & Timeline
4.15	Local court administrators are responsible to ensure that local applications loaded on court-supported desktop/laptop systems are patched and that no security vulnerabilities exist.				
4.16	No device residing on the court's network has dual access to a non-court network without being approved and configured by the AOC.				
4.17	All network equipment used to grant access onto the court network is the responsibility of the local technology organization. This includes, but is not limited to, routers, switches, and access points.				
4.18	Any use of network monitoring tools on the court network is approved by the information technology manager prior to use. Data capturing tools are prohibited on AJIN.				
4.19	The laws for copyrights, patents, trademarks, and the like are enforced as stated in the Arizona Judicial Department Electronic Communication Policy. Copying of pirated or bootleg software is strictly prohibited.				